UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/617,465	07/11/2003	Mark L. Buer	2875.0370001	5029

26111 7590 07/25/2007
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
07/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/617,465	BUER ET AL.	
	Examiner	Art Unit	
	Carlton V. Johnson	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 4-27-2007.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-42 is/are pending in the application.

4a) Of the above claim(s) 5,7-13,18,20-27,30 and 31 is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-4,6,14-17,19,28, 29,32-42 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed **4-27-2007**.

2. Claims **1 - 42** are pending. Claims **1, 14, 28** have been amended. Claims **5, 7 - 13, 18, 20 - 27, 30, 31** have been canceled. Claims **32 - 42** are new. Claims **1, 14, 28, 39** are independent.

Response to Remarks

3 The following is in response to papers filed on 4-27-2007.

3.1 Applicant argues that the claim limitations stated within the amendments to claims are not disclosed. The claims amendments are addressed in the accompanying Office Action.

3.2 The examiner has considered the applicant's remarks concerning a system for providing secured data transmission over a data network using security association information. Before encryption, the system calculates values for header fields that need to be updated as a result of an encryption process. After decryption, the system calculates values for fields in the header information that need to be updated as a result of the decryption process. Applicant's arguments have thus been fully analyzed and considered but they are not persuasive

After an additional analysis of the applicant's invention, remarks, and a search of the available prior art, it was determined that the current set of prior art consisting of

Noehring (**20020188839**) discloses applicant's invention including disclosures in Remarks dated April 27, 2007.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102(e) that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims **1 - 4, 6, 14 - 17, 19, 28, 29, 32 - 42** are rejected under 35 U.S.C. 102(e) as being anticipated by **Noehring et al.** (US PGPUB No. **20020188839**).

Regarding Claim 1, Noehring discloses a packet processing method comprising:

a) receiving a plurality of packets; (see Noehring paragraph [0033], lines 3-5: multiple packets processed)

b) receiving a security association handle for each packet in the plurality of packets, wherein the security association handle includes a set of selectors; (see Noehring paragraph [00045], lines 7-10; paragraph [0051], lines 1-3: tag (handle) appended to each packet)

c) for each packet, identifying a flow entry for the packet, including:

d) determining a flow element address for the packet, (see Noehring paragraph

[0051], lines 1-3: pointer (address) for SAD entry)

e) retrieving a first flow element using the flow element address, wherein the first flow element includes a plurality of flow entries, (see Noehring paragraph [0052], lines 1-4: channel (flow element) selected for packet processing)

f) determining whether a selector in the set of security association handle selectors is present in one of the plurality of flow entries, (see Noehring paragraph [0047], lines 11-18: determination selector (addresses, ports) information in security association structure) and

g) retrieving a second flow element if a selector in the set of security association handle selectors is not present in one of the plurality of flow entries; (see Noehring paragraph [0052], lines 1-4: channel (flow entry) selected for packet)

h) retrieving security association information for each packet using the identified flow entry; (see Noehring paragraph [0053], lines 1-3: retrieve SAD entry with appended tag (handle))

i) generating header information for each of the plurality of packets; (see Noehring paragraph [0030], lines 5-7: generate header)

j) adding the header information to each of the plurality of packets to generate encapsulated packets; (see Noehring paragraph [0011], lines 12-15: add header) and

k) distributing the encapsulated packets to a plurality of cryptographic processors. (see Noehring paragraph [0007], lines 1-3; paragraph [0007], lines 4-8;

paragraph [0036], lines 1-2; paragraph [0036], lines 8-12: distribute encapsulated packet, multiple processors (i.e. encryption processors, RISC processors), encryption of packets)

Regarding Claim 2, Noehring discloses the method of claim 1 wherein the information comprises one or more of the group consisting of sequence number and byte count. (see Noehring paragraph [0030], lines 4-5: information, sequence number)

Regarding Claim 3, Noehring discloses the method of claims 1 wherein the encapsulated packets comprise IPsec packets. (see Noehring paragraph [0044], lines 18-20: encapsulation, IPSec packets utilized)

Regarding Claim 4, Noehring discloses the method of claims 1 wherein packets are encapsulated on a per-packet basis. (see Noehring paragraph [0044], lines 18-20: processing each packet)

Regarding Claim 6, Noehring discloses the method of claims 1 wherein the packets are received from a host processor. (see Noehring paragraph [0043], lines 17-19: host processor)

Regarding Claims 14, Noehring discloses a packet processing method comprising:

a) receiving a plurality of encrypted packets comprising header information and encrypted data; (see Noehring paragraph [0033], lines 3-5: multiple packets processed; paragraph [0031], lines 5-7: encrypted packets received (inbound))

b) receiving a security association handle for each packet in the plurality of packets, wherein the security association handle includes a set of selectors; (see Noehring paragraph [00045], lines 7-10; paragraph [0051], lines 1-3: tag (handle) appended to each packet)

c) for each packet, identifying a flow entry for the packet, including:

d) determining a flow element address for the packet, (see Noehring paragraph [0051], lines 1-3: pointer (address) for SAD entry)

e) retrieving a first flow element using the flow element address, wherein the first flow element includes a plurality of flow entries, (see Noehring paragraph [0052], lines 1-4: channel (flow element) selected for packet)

f) determining whether a selector in the set of security association handle selectors is present in one of the plurality of flow entries, (see Noehring paragraph [0047], lines 11-18: determination selector (addresses, ports) information in security association structure) and

g) retrieving a second flow element if a selector in the set of security association handle selectors is not present in one of the plurality of flow entries; (see Noehring paragraph [0052], lines 1-4: channel (flow entry) selected for packet)

h) retrieving security association information for each packet using the identified flow entry; (see Noehring paragraph [0053], lines 1-3: retrieve SAD entry with appended tag (handle))

i) distributing the packets to a plurality of cryptographic processors; (see Noehring paragraph [0007], lines 1-3; paragraph [0007], lines 4-8; paragraph [0036], lines 1-2; paragraph [0036], lines 8-12: multiple processors (i.e. encryption, cryptographic processors), distribute encapsulated packet, concurrent encryption on multiple packets)

j) decrypting the encrypted portion of each packet based on a portion of the security association information retrieved for the packet; (see Noehring paragraph [0031], lines 5-7; paragraph [0039], lines 1-4: decryption of packets)

k) modifying, by a common processing component, at least a portion of the header information of the decrypted packets; (see Noehring paragraph [0030], lines 1-7: update (i.e. modify) sequence number, a portion of header information) and

l) transmitting the decrypted packets. (see Noehring paragraph [0027], lines 24-28: output packets)

Regarding Claims 15, 29, Noehring discloses the method, packet processing system of claims 14, 28 wherein the at least a portion of the security association information comprises one or more of the group consisting of sequence number and byte count. (see Noehring paragraph [0030], lines 4-5: information, sequence number)

Regarding Claims 16, Noehring discloses the method of claim 14 wherein the encrypted packets comprise IPsec packets. (see Noehring paragraph [0027], lines 16-20: IPSec packet processing; paragraph [0031], lines 1-5: encryption)

Regarding Claims 17, Noehring discloses the method of claim 14 wherein the at least a portion of the header information is modified on a per-packet basis. (see Noehring paragraph [0030], lines 1-7: update (i.e. modify) portion of header information; paragraph [0006], lines 3-16: processing on a per-packet basis)

Regarding Claims 19, Noehring discloses the method of claim 14 wherein the packets are transmitted to a host processor. (see Noehring paragraph [0043], lines 17-19: host processor)

Regarding Claims 28, Noehring discloses a packet processing system comprising:

a) at least one media access controller for receiving a plurality of packets; (see Noehring paragraph [0033], lines 3-5: multiple packets processed)

b) at least one data memory for storing security association information; (see Noehring see Noehring paragraph [0028], lines 12-16; paragraph [0047], lines 1-4; paragraph [0047], lines 14-18: database, security association information) and

c) <u>a cryptographic processing module</u> (see Noehring paragraph [0007], lines 1-3; paragraph [0007], lines 4-8; paragraph [0036], lines 1-2; paragraph [0036], lines

8-12: multiple processors (i.e. encryption, cryptographic processors), distribute encapsulated packet, concurrent encryption on multiple packets),

wherein the cryptographic processing module includes:

b) a policy lookup unit configured to identify a flow associated with each of the received plurality of packets and to retrieve a security association for each identified flow; (see Noehring paragraph [0057], lines 1-4: security policy index (lookup capability))

c) a merge data unit coupled to the policy lookup unit configured to merge a portion of the security association retrieved by the policy lookup unit with the associated packet, (see Noehring paragraph [0057], lines 1-4; merged, security association and policy lookup data)

d) a plurality of cryptographic processors, each coupled to the merged data unit for performing cryptographic operations on the merged packets. (see Noehring paragraph [0007], lines 1-3; paragraph [0007], lines 4-8; paragraph [0036], lines 1-2; paragraph [0036], lines 8-12: multiple processors (i.e. encryption, cryptographic processors), distribute encapsulated packet, concurrent encryption on multiple packets)

Regarding Claim 32, Noehring discloses the method of claim 1, wherein determining a flow element address includes: hashing the selectors in the set of security association handle selectors to generate the flow element address. (see Noehring paragraph [00045], lines 7-10; paragraph [0051], lines 1-3: security association tag (handle) appended to each packet; paragraph [0039], lines 1-4; paragraph [0059], lines 2-6: hash capability)

Regarding Claim 33, Noehring discloses the method of claim 1, wherein the step of determining a flow element address includes:

a) retrieving a security parameter index from the set of security association handle selectors; (see Noehring paragraph [0057], lines 1-4: retrieve security policy (security parameter) index) and

b) using the retrieved security parameter index as the flow element address. (see Noehring paragraph [0051], lines 1-3; col. 52, lines 1-4: channel selection for flow)

Regarding Claim 34, Noehring discloses the method of claim 1, further comprising:

a) processing each encapsulated packet based on the retrieved security association information for the packet; (see Noehring paragraph [0060], lines 9-15: process packet based on security information) and

b) transmitting the processed packet. (see Noehring paragraph [0063], lines 1-6: transmit processed packet)

Regarding Claim 35, Noehring discloses the method of claim 1, further comprising:

a) modifying a least a portion of the retrieved security association information; (see Noehring paragraph [0057], lines 8-11: modify security association information) and

b) generating header information for the packets including a portion of the modified security association information. (see Noehring paragraph [0057], lines 4-8: generate header information, security association information)

Regarding Claim 36, Noehring discloses the method of claim 14, wherein determining a flow element address includes: hashing the selectors in the set of security association handle selectors to generate the flow element address. (see Noehring paragraph [0039], lines 1-4; paragraph [0059], lines 2-6: hash generation capabilities)

Regarding Claim 37, Noehring discloses the method of claim 14, wherein the step of determining a flow element address includes:

a) retrieving a security parameter index from the set of security association handle selectors; (see Noehring paragraph [0057], lines 1-4: retrieve security policy (security parameter) index) and

b) using the retrieved security parameter index as the flow element address. (see Noehring paragraph [0051], lines 1-3; col. 52, lines 1-4: channel selection for flow)

Regarding Claim 38, Noehring discloses the packet processing system of claim 28, wherein the cryptographic processing module further comprises: a distributor coupled between the merge data unit and the plurality cryptographic processors for distributing merged packets to the plurality of cryptographic processors. (see Noehring paragraph [0057], lines 1-4: merged packets (policy and association information; paragraph [0007], lines 1-3; paragraph [0007], lines 4-8; paragraph [0036], lines 1-2; paragraph [0036], lines 8-12: multiple processors (i.e. encryption, cryptographic processors), distribute encapsulated packet, concurrent encryption on multiple packets)

Regarding Claim 39, Noehring discloses a method for determining security association information in a cryptographic processor comprising:

a) receiving a security association handle for a packet, wherein the security association handle includes a set of selectors; (see Noehring paragraph [00045], lines 7-10; paragraph [0051], lines 1-3: tag (handle) appended to each packet)

b) determining a flow element address for the packet; (see Noehring paragraph [0051], lines 1-3: pointer (address) for SAD entry)

c) retrieving a first flow element using the flow element address, wherein the first flow element includes a plurality of flow entries; (see Noehring paragraph [0052], lines 1-4: channel (flow element) selected for packet)

d) identifying a flow entry having a selector matching a selector in the set of security association handle selectors; (see Noehring paragraph [0054], lines 1-3: check SAD entry for match)

e) retrieving security association information using the identified flow entry; (see Noehring paragraph [0053], lines 1-3: retrieve SAD entry with appended tag (handle)) and

f) transmitting at least a portion of the retrieved security association information to a cryptographic processing engine. (see Noehring paragraph [0060], lines 9-15: security association information used to process packet)

Regarding Claim 40, Noehring discloses the method of claim 39, further comprising: retrieving a second flow element if a selector in the set of security association handle selectors is not present in one of the plurality of flow entries. (see Noehring paragraph [0052], lines 1-4: channel (flow element) selected for packet)

Regarding Claim 41, Noehring discloses the method of claim 39, wherein determining a flow element address includes: hashing the selectors in the set of security association handle selectors to generate the flow element address. (see Noehring paragraph [0052], lines 1-4: channel selected (flow element address); paragraph [0039], lines 1-4; paragraph [0059], lines 2-6: hash generation capabilities)

Regarding Claim 42, Noehring discloses the method of claim 39, wherein the step of determining a flow element address includes:

a) retrieving a security parameter index from the set of security association handle selectors; (see Noehring paragraph [0057], lines 1-4: retrieve security policy (security parameter) index)) and

b) using the retrieved security parameter index as the flow element address. (see Noehring paragraph [0051], lines 1-3; col. 52, lines 1-4: channel selection for flow)

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-

270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

7/23/07

C.J.
CVJ
July 9, 2007